https://doi.org/10.1145/3652029

Applied Machine Learning for Information Security

SAGAR SAMTANI

Indiana University, Bloomington, United States, ssamtani@iu.edu

EDWARD RAFF

Booz Allen Hamilton, University of Maryland, Baltimore County, edraff1@umbc.edu

HYRUM ANDERSON

Robust Intelligence, Boise, United States, hyrum@robustintelligence.com

Information security has undoubtedly become a critical aspect of modern cybersecurity practices. Over the last half-decade, numerous academic and industry groups have sought to develop machine learning, deep learning, and other areas of artificial intelligence-enabled analytics into information security practices. The Conference on Applied Machine Learning (CAMLIS) is an emerging venue that seeks to gather researchers and practitioners to discuss applied and fundamental research on machine learning for information security applications. In 2021, CAMLIS partnered with *ACM Digital Threats: Research and Practice (DTRAP)* to provide opportunities for authors of accepted CAMLIS papers to submit their research for consideration into *ACM DTRAP* via a Special Issue on Applied Machine Learning for Information Security. This editorial summarizes the results of this Special Issue.

CCS CONCEPTS • Security and Privacy • Machine Learning • Artificial Intelligence

Additional Keywords and Phrases: applied machine learning, deep learning, artificial intelligence, information security, cybersecurity

1 INTRODUCTION

Artificial Intelligence (AI)-enabled analytics based on machine learning, deep learning, large language models, network science, and other methodologies have played a pivotal role in revolutionizing numerous industries. Information security professionals are increasingly employing AI-enabled analytics for many different tasks, including cyber threat intelligence [32,43,56], vulnerability management [1,16,19,21,23,28,29,44,54,55,57], Dark Web analytics [2–4,13,18,22,24–27,30,31,33,35–38,45,51,58], malware and phishing analysis [5,10,11,39,40,59], adversarial attack emulation and evasion [6–9,15,17,20,34,42,53], and more. Indeed, numerous past scholars and practitioners have noted AI-enabled analytics' role in improving information security applications [12,14,46–50]. Although there is clear practical guidance on how to execute selected areas of AI-enabled analytics (e.g., deep learning [41,52]) significant efforts are needed to coalesce groups of practitioners and academics working in these areas.

The Conference on Applied Machine Learning for Information Security (CAMLIS) has emerged as a prevailing venue for practitioners and academics to share ideas and emerging research related to various aspects of AI-enabled cybersecurity analytics, particularly those focused on information security topics. Conceived and launched originally in 2017 and held annually in Washington, DC, CAMLIS has rapidly grown in visibility. In 2021, authors who submitted to CAMLIS were offered an opportunity to submit to a special issue on the topic at *ACM Digital Threats: Research and Practice*

ACM 2692-1626/2024/03-ART
http://dx.doi.org/10.1145/3652029

(DTRAP). The remainder of this editorial details the process for submissions and the papers included in this special issue.

2 INSIDE THIS SPECIAL ISSUE

Authors for the 2021 iteration of CAMLIS was held on November 4-5, 2021 at the Sands Capital Management. were offered two opportunities to submit their work to the conference: (1) a full length paper for consideration as a talk or (2) an abstract. At the end of the conference, all attendees were notified about the possible opportunity to submit to the special issue at *ACM DTRAP*. The call for papers invited authors who submitted their papers to CAMLIS 2021 or 2022 to submit their work, as well as others who had work related to the topic of the special issue. In total, 15 manuscripts were received. Each paper was assigned to three reviewers for their assessment and feedback. All conflicts of interest were carefully managed. Final decisions on the manuscripts were made by the two Editors in Chiefs of *ACM DTRAP*.

The accepted manuscripts had excellent coverage across a broad range of information security applications in which machine learning, deep learning, and other analytics techniques could be leveraged. In the article "Improving Automated Labeling for ATT&CK Tactics in Malware Threat Reports," the authors sought to employ techniques to map malware-related content from threat reports to a prevailing cybersecurity risk management framework. The article "ANDROIDGYNY: Reviewing clustering techniques for Android malware family classification" provided an overview of the state-of-the-art ML approaches that could be leveraged for Android malware analysis. Malware analysis was also represented in the article "Efficient Malware Analysis Using Metric Embeddings," which sought to optimize the efficiency of common malware processing through innovative embedding perspectives. In the article "Towards Attack Detection in Multimodal Cyber-Physical Systems with Sticky HDP-HMM based Time Series Analysis," the authors sought to take a temporal modeling perspective on multi-modal data to detect attacks on various cyber-physical systems. The special issue also included perspectives on identifying and modeling vulnerabilities within systems. For instance, the article "Asm2Seq: Explainable Assembly Code Functional Summary Generation for Reverse Engineering and Vulnerability Analysis" sought to represent assembly code summaries effectively through various encoder-decoder structures. In the article "Evading Anti-Phishing Models: A Field Note Documenting an Experience in the Machine Learning Security Evasion Competition 2022," the authors reported on their experiences perturbing phishing websites to evade various phishing websites. In the article "Enhancements to Threat, Vulnerability and Mitigation Knowledge for Cyber Analytics, Hunting, and Simulations," the authors sought to build upon their research stream to help enable effective threat-hunting capabilities. In the article entitled "Locally and Structurally Private Graph Neural Networks," the authors sought to help improve the robustness of popular graph embedding approaches. Finally, the article "Machine Learning (In) Security: A Stream of Problems" sought to effectively summarize prevailing security issues commonly seen in ML models. We hope that the readers of this issue enjoy reading the accepted articles.

ACKNOWLEDGMENTS

We are grateful to all of the reviewers who spent time assessing the submitted manuscripts. We appreciate all the guidance provided by the ACM DTRAP EICs. This work was supported in part by the National Science Foundation Grant Nos. CNS-2338479 (SaTC CAREER), DGE-1946537 (SFS), OAC-2319325 (CICI), and OAC-197117 (CICI).

3 HISTORY DATES

Received March 2024; revised March 2024; accepted March 2024

REFERENCES

[1] B. Ampel, S. Samtani, S. Ullman, and H. Chen. 2021. Linking common vulnerabilities and exposures to the mitre ATT&CK framework: A self-distillation approach. In *ACM KDD Workshop on AI-enabled Analytics for Cybersecurity*, arxiv.org, 1–6. Retrieved from http://arxiv.org/abs/2108.01696

[2] Benjamin Ampel and Hsinchun Chen. 2021. Distilling Contextual Embeddings Into A Static Word Embedding For Improving Hacker Forum Analytics. In *2021 IEEE International Conference on Intelligence and Security Informatics (ISI)*, ieeexplore.ieee.org, 1–3. DOI:https://doi.org/10.1109/ISI53945.2021.9624848

[3] Benjamin M. Ampel, Sagar Samtani, Hongyi Zhu, Hsinchun Chen, and Jay F. Nunamaker Jr. 2024. Improving Threat Mitigation Through a Cybersecurity Risk Management Framework: A Computational Design Science Approach. *Journal of Management Information Systems* 41, 1 (January 2024), 236–265. DOI:https://doi.org/10.1080/07421222.2023.2301178

[4] Benjamin Ampel, Sagar Samtani, Hongyi Zhu, Steven Ullman, and Hsinchun Chen. 2020. Labeling Hacker Exploits for Proactive Cyber Threat Intelligence: A Deep Transfer Learning Approach. In *2020 IEEE International Conference on Intelligence and Security Informatics (ISI)*, 1–6. DOI:https://doi.org/10.1109/ISI49825.2020.9280548

[5] H. S. Anderson and P. Roth. 2018. Ember: an open dataset for training static pe malware machine learning models. *arXiv preprint arXiv:1804.04637* (2018). Retrieved from http://arxiv.org/abs/1804.04637

[6] G. Apruzzese, M. Andreolini, and M. Colajanni. 2020. Hardening random forest cyber detectors against adversarial attacks. *on Emerging Topics …* (2020). Retrieved from https://ieeexplore.ieee.org/abstract/document/9099383/

[7] G. Apruzzese, M. Andreolini, and L. Ferretti. 2022. Modeling realistic adversarial attacks against network intrusion detection systems. *Threats: Research and …* (2022). Retrieved from https://dl.acm.org/doi/abs/10.1145/3469659

[8] G. Apruzzese, M. Andreolini, and M. Marchetti. 2020. Deep reinforcement adversarial learning against botnet evasion attacks. *on Network and …* (2020). Retrieved from https://ieeexplore.ieee.org/abstract/document/9226405/

[9] G. Apruzzese, M. Colajanni, and L. Ferretti. 2019. Addressing adversarial attacks against security systems based on machine learning. *Conf. Proc. IEEE Int. Conf. Syst. Man Cybern.* (2019). Retrieved from https://ieeexplore.ieee.org/abstract/document/8756865/

[10] G. Apruzzese, M. Conti, and Y. Yuan. 2022. SpacePhish: The Evasion-space of Adversarial Attacks against Phishing Website Detectors using Machine Learning. *of the 38th Annual Computer Security …* (2022). Retrieved from https://dl.acm.org/doi/abs/10.1145/3564625.3567980

[11] G. Apruzzese and V. S. Subrahmanian. 2022. Mitigating Adversarial Gray-Box Attacks Against Phishing Detectors. *IEEE Transactions on* (2022). Retrieved from https://ieeexplore.ieee.org/abstract/document/9904297/

[12] Giovanni Apruzzese, Pavel Laskov, Edgardo Montes de Oca, Wissam Mallouli, Luis Brdalo Rapa, Athanasios Vasileios Grammatopoulos, and Fabio Di Franco. 2023. The Role of Machine Learning in Cybersecurity. *Digital Threats* 4, 1 (March 2023), 1–38. DOI:https://doi.org/10.1145/3545574

[13] V. Benjamin, J. S. Valacich, and H. Chen. 2019. DICE-E: A Framework for Conducting Darknet Identification, Collection, Evaluation with Ethics. *MIS Quarterly* 43, 1 (2019), 1–22. DOI:https://doi.org/10.25300/MISQ/2019/13808

[14] Elisa Bertino, Murat Kantarcioglu, Cuneyt Gurcan Akcora, Sagar Samtani, Sudip Mittal, and Maanak Gupta. 2021. AI for Security and Security for AI. In *Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy* (CODASPY '21), Association for Computing Machinery, New York, NY, USA, 333–334. DOI:https://doi.org/10.1145/3422337.3450357

[15] Yidong Chai, Ruicheng Liang, Sagar Samtani, Hongyi Zhu, Meng Wang, Yezheng Liu, and Yuanchun Jiang. 2023. Additive feature attribution explainable methods to craft adversarial attacks for text classification and text regression. *IEEE Trans. Knowl. Data Eng.* (2023), 1–14. DOI:https://doi.org/10.1109/tkde.2023.3270581

[16] Haipeng Chen, Andrew Duncklee, Sushil Jajodia, Rui Liu, Sean Mcnamara, and V. S. Subrahmanian. 2022. PCAM: A Data-driven Probabilistic Cyber-alert Management Framework. *ACM Trans. Internet Technol.* 22, 3 (January 2022), 1–24. DOI:https://doi.org/10.1145/3511101

[17] Mohammadreza Ebrahimi, Sagar Samtani, Yidong Chai, and Hsinchun Chen. 2020. Detecting cyber threats in non-English hacker forums: An adversarial cross-lingual knowledge transfer approach. In *2020 IEEE Security and Privacy Workshops (SPW)*, 20–26. DOI:https://doi.org/10.1109/SPW50608.2020.00021

[18] Mohammedreza Ebrahimi, Yidong Chai, Sagar Samtani, and Hsinchun Chen. 2022. Cross-lingual cybersecurity analytics in the international dark web with adversarial deep representation learning. *MIS Quarterly* 46, 2 (2022), 1209–1226. DOI:https://doi.org/10.25300/MISQ/2022/16618

[19] Katheryn A. Farris, Ankit Shah, George Cybenko, Rajesh Ganesan, and Sushil Jajodia. 2018. VULCON: A System for Vulnerability Prioritization, Mitigation, and Management. *ACM Trans. Priv. Secur.* 21, 4 (June 2018), 1–28. DOI:https://doi.org/10.1145/3196884

[20] W. Fleshman, E. Raff, J. Sylvester, and S. Forsyth. 2018. Non-negative networks against adversarial attacks. *arXiv preprint arXiv* (2018). Retrieved from https://arxiv.org/abs/1806.06108

[21] Rajesh Ganesan, Sushil Jajodia, Ankit Shah, and Hasan Cam. 2016. Dynamic Scheduling of Cybersecurity Analysts for Minimizing Risk Using Reinforcement Learning. *ACM Trans. Intell. Syst. Technol.* 8, 1 (July 2016), 1–21. DOI:https://doi.org/10.1145/2882969

[22] John Grisham, Sagar Samtani, Mark Patton, and Hsinchun Chen. 2017. Identifying mobile malware and key threat actors in online hacker forums for proactive cyber threat intelligence. In *2017 IEEE International Conference on Intelligence and Security Informatics (ISI)*, 13–18. DOI:https://doi.org/10.1109/ISI.2017.8004867

[23] C. R. Harrell, M. Patton, and H. Chen. 2018. Vulnerability assessment, remediation, and automated reporting: Case studies of higher education institutions. *2018 IEEE International* (2018). Retrieved from https://ieeexplore.ieee.org/abstract/document/8587380/

[24] Jack Hughes, Seth Aycock, Andrew Caines, Paula Buttery, and Alice Hutchings. 2020. Detecting Trending Terms in Cybersecurity Forum Discussions. In *Proceedings of the Sixth Workshop on Noisy User-generated Text (W-NUT 2020)*, Association for Computational Linguistics, Online, 107–115. DOI:https://doi.org/10.18653/v1/2020.wnut-1.15

[25] Jack Hughes, Ben Collier, and Alice Hutchings. 2019. From playing games to committing crimes: A multi-technique approach to predicting key actors on an online gaming forum. In *2019 APWG Symposium on Electronic Crime Research (eCrime)*, IEEE. DOI:https://doi.org/10.1109/ecrime47957.2019.9037586

[26] Jack Hughes, Sergio Pastrana, Alice Hutchings, Sadia Afroz, Sagar Samtani, Weifeng Li, and Ericsson Santana Marin. 2024. The Art of Cybercrime Community Research. *ACM Comput. Surv.* 56, 6 (February 2024), 1–26. DOI:https://doi.org/10.1145/3639362

[27] Youngjin Jin, Eugene Jang, Jian Cui, Jin-Woo Chung, Yongjae Lee, and Seungwon Shin. 2023. DarkBERT: A Language Model for the Dark Side of the Internet. *arXiv [cs.CL]*. DOI:https://doi.org/10.48550/arXiv.2305.08596

[28] Ben Lazarine, Sagar Samtani, Mark Patton, Hongyi Zhu, Steven Ullman, Benjamin Ampel, and Hsinchun Chen. 2020. Identifying Vulnerable GitHub Repositories and Users in Scientific Cyberinfrastructure: An Unsupervised Graph Embedding Approach. In *2020 IEEE International Conference on Intelligence and Security Informatics (ISI)*, 1–6. DOI:https://doi.org/10.1109/ISI49825.2020.9280544

[29] Ben Lazarine, Zhong Zhang, Agrim Sachdeva, Sagar Samtani, and Hongyi Zhu. 2022. Exploring the Propagation of Vulnerabilities from GitHub Repositories Hosted by Major Technology Organizations. In *Proceedings of the 15th Workshop on Cyber Security Experimentation and Test* (CSET '22), Association for Computing Machinery, New York, NY, USA, 145–150. DOI:https://doi.org/10.1145/3546096.3546114

[30] Weifeng Li and Hsinchun Chen. 2022. Discovering emerging threats in the hacker community: A nonparametric emerging topic detection framework. *MIS Quarterly* 46, 4 (December 2022), 2337–2350. DOI:https://doi.org/10.25300/misq/2022/15642

[31] Fangyu Lin, Yizhi Liu, Mohammadreza Ebrahimi, Zara Ahmad-Post, James Lee Hu, Jingyu Xin, Sagar Samtani, Weifeng Li, and Hsinchun Chen. 2020. Linking personally identifiable information from the dark web to the surface web: A deep entity resolution approach. In *2020 International Conference on Data Mining Workshops (ICDMW)*, IEEE. DOI:https://doi.org/10.1109/icdmw51313.2020.00072

[32] Manatova, Camp, Fox, Kuebler, Shardakova, and Kouper. 2023. An Argument for Linguistic Expertise in Cyberthreat Analysis: LOLSec in Russian Language eCrime Landscape. In *2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, computer.org, 170–176. DOI:https://doi.org/10.1109/EuroSPW59978.2023.00024

[33] Dalyapraz Manatova, Dewesha Sharma, Sagar Samtani, and L. Jean Camp. 2022. Building and Testing a Network of Social Trust in an Underground Forum: Robust Connections and Overlapping Criminal Domains. In *2022 APWG Symposium on Electronic Crime Research (eCrime)*, 1–12. DOI:https://doi.org/10.1109/eCrime57793.2022.10142120

[34] A. T. Nguyen and E. Raff. 2018. Adversarial attacks, regression, and numerical stability regularization. *arXiv preprint arXiv:1812.02885* (2018). Retrieved from http://arxiv.org/abs/1812.02885

[35] Kaeli Otto, Benjamin Ampel, Sagar Samtani, Hongyi Zhu, and Hsinchun Chen. 2021. Exploring the Evolution of Exploit-Sharing Hackers: An Unsupervised Graph Embedding Approach. In *2021 IEEE International Conference on Intelligence and Security Informatics (ISI)*, ieeexplore.ieee.org, 1–6. DOI:https://doi.org/10.1109/ISI53945.2021.9624846

[36] Kaeli Otto, Benjamin Ampel, Sagar Samtani, Hongyi Zhu, and Hsinchun Chen. 2021. Exploring the Evolution of Exploit-Sharing Hackers: An Unsupervised Graph Embedding Approach. In *2021 IEEE International Conference on Intelligence and Security Informatics (ISI)*, IEEE, 1–6. DOI:https://doi.org/10.1109/ISI53945.2021.9624846

[37] Ildiko Pete, Jack Hughes, Andrew Caines, Anh V. Vu, Harshad Gupta, Alice Hutchings, Ross Anderson, and Paula Buttery. 2022. PostCog: A tool for interdisciplinary research into underground forums at scale. In *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, IEEE, 93–104. DOI:https://doi.org/10.1109/EuroSPW55150.2022.00016

[38] Ildiko Pete, Jack Hughes, Yi Ting Chua, and Maria Bada. 2020. A social network analysis and comparison of six dark web forums. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, IEEE. DOI:https://doi.org/10.1109/eurospw51379.2020.00071

[39] E. Raff, W. Fleming, R. Zak, and H. Anderson. 2019. Kilograms: Very large n-grams for malware classification. *arXiv preprint arXiv* (2019). Retrieved from https://arxiv.org/abs/1908.00200

[40] E. Raff and C. Nicholas. 2020. A survey of machine learning methods and challenges for windows malware classification. *arXiv preprint arXiv:2006.09271* (2020). Retrieved from http://arxiv.org/abs/2006.09271

[41] Edward Raff. 2022. *Inside Deep Learning: Math, Algorithms, Models*. Manning. Retrieved from https://play.google.com/store/books/details?id=s8hhzgEACAAJ

[42] Colin Raffel, Noam Shazeer, Adam Roberts, Katherine Lee, Sharan Narang, Michael Matena, Yanqi Zhou, Wei Li, and Peter J. Liu. 2020. Exploring the limits of transfer learning with a unified text-to-text transformer. *J. Mach. Learn. Res.* 21, 1 (January 2020), 5485–5551. Retrieved from https://dl.acm.org/doi/abs/10.5555/3455716.3455856

[43] Md Rayhanur Rahman, Rezvan Mahdavi Hezaveh, and Laurie Williams. 2023. What Are the Attackers Doing Now? Automating Cyberthreat Intelligence Extraction from Text on Pace with the Changing Threat Landscape: A Survey. *ACM Comput. Surv.* 55, 12 (March 2023), 1–36. DOI:https://doi.org/10.1145/3571726

[44] Agrim Sachdeva, Ben Lazarine, Hongyi Zhu, and Sagar Samtani. 2023. User Profiling and Vulnerability Introduction Prediction in Social Coding Repositories: A Dynamic Graph Embedding Approach: Vulnerability Introduction Prediction in Social Coding Repositories. In *Proceedings of the 16th Cyber Security Experimentation and Test Workshop* (CSET '23), Association for Computing Machinery, New York, NY, USA, 19–25. DOI:https://doi.org/10.1145/3607505.3607512

[45] Sagar Samtani, Yidong Chai, and Hsinchun Chen. 2022. Linking Exploits from the Dark Web to Known Vulnerabilities for Proactive Cyber Threat Intelligence: An Attention-Based Deep Structured Semantic Model. *MIS Quarterly* 46, 2 (2022), 911–946. DOI:https://doi.org/10.25300/MISQ/2022/15392

[46] Sagar Samtani, Hsinchun Chen, Murat Kantarcioglu, and Bhavani Thuraisingham. 2022. Explainable Artificial Intelligence for Cyber Threat Intelligence (XAI-CTI). *IEEE Trans. Dependable Secure Comput.* 19, 4 (July 2022), 2149–2150. DOI:https://doi.org/10.1109/TDSC.2022.3168187

[47] Sagar Samtani, Murat Kantarcioglu, and Hsinchun Chen. 2020. Trailblazing the Artificial Intelligence for Cybersecurity Discipline: A Multi-Disciplinary Research Roadmap. *ACM Trans. Manage. Inf. Syst.* 11, 4 (December 2020), 1–19. DOI:https://doi.org/10.1145/3430360

[48] Sagar Samtani, Gang Wang, Ali Ahmadzadeh, Arridhana Ciptadi, Shanchieh Yang, and Hsinchun Chen. 2022. ACM KDD AI4Cyber/MLHat: Workshop on AI-enabled Cybersecurity Analytics and Deployable Defense. In *Proceedings of the 28th ACM SIGKDD Conference on Knowledge Discovery and Data Mining* (KDD '22), Association for Computing Machinery, New York, NY, USA, 4900–4901. DOI:https://doi.org/10.1145/3534678.3542894

[49] Sagar Samtani, Shanchieh Yang, and Hsinchun Chen. 2021. ACM KDD AI4Cyber: The 1st Workshop on Artificial Intelligence-enabled Cybersecurity Analytics. In *Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining* (KDD '21), Association for Computing Machinery, New York, NY, USA, 4153–4154. DOI:https://doi.org/10.1145/3447548.3469450

[50] Sagar Samtani, Ziming Zhao, and Ram Krishnan. 2023. Secure Knowledge Management and Cybersecurity in the Era of Artificial Intelligence. *Inf. Syst. Front.* 25, 2 (February 2023), 425–429. DOI:https://doi.org/10.1007/s10796-023-10372-y

[51] Sagar Samtani, Hongyi Zhu, and Hsinchun Chen. 2020. Proactively Identifying Emerging Hacker Threats from the Dark Web: A Diachronic Graph Embedding Framework (D-GEF). *ACM Trans. Priv. Secur.* 23, 4 (August 2020), 1–33. DOI:https://doi.org/10.1145/3409289

[52] Sagar Samtani, Hongyi Zhu, Balaji Padmanabhan, Yidong Chai, Hsinchun Chen, and Jay F. Nunamaker. 2023. Deep Learning for Information Systems Research. *Journal of Management Information Systems* 40, 1 (January 2023), 271–301. DOI:https://doi.org/10.1080/07421222.2023.2172772

[53] J. Schneider and G. Apruzzese. 2022. Concept-based adversarial attacks: Tricking humans and classifiers alike. *2022 IEEE Security and Privacy* (2022). Retrieved from https://ieeexplore.ieee.org/abstract/document/9833874/

[54] Ankit Shah, Katheryn A. Farris, Rajesh Ganesan, and Sushil Jajodia. 2022. Vulnerability Selection for Remediation: An Empirical Analysis. *Journal of Defense Modeling & Simulation* 19, 1 (January 2022), 13–22. DOI:https://doi.org/10.1177/1548512919874129

[55] Ankit Shah, Rajesh Ganesan, Sushil Jajodia, and Hasan Cam. 2022. Maintaining the level of operational effectiveness of a CSOC under adverse conditions. *Int. J. Inf. Secur.* 21, 3 (June 2022), 637–651. DOI:https://doi.org/10.1007/s10207-021-00573-4

[56] Nan Sun, Ming Ding, Jiaojiao Jiang, Weikang Xu, Xiaoxing Mo, Yonghang Tai, and Jun Zhang. 2023. Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives. *IEEE Communications Surveys & Tutorials* (2023), 1–1. DOI:https://doi.org/10.1109/COMST.2023.3273282

[57] Steven Ullman, Sagar Samtani, Ben Lazarine, Hongyi Zhu, Benjamin Ampel, Mark Patton, and Hsinchun Chen. 2020. Smart Vulnerability Assessment for Scientific Cyberinfrastructure: An Unsupervised Graph Embedding Approach. In *2020 IEEE International Conference on Intelligence and Security Informatics (ISI)*, 1–6. DOI:https://doi.org/10.1109/ISI49825.2020.9280545

[58] Tala Vahedi, Benjamin Ampel, Sagar Samtani, and Hsinchun Chen. 2021. Identifying and Categorizing Malicious Content on Paste Sites: A Neural Topic Modeling Approach. In *2021 IEEE International Conference on Intelligence and Security Informatics (ISI)*, ieeexplore.ieee.org, 1–6. DOI:https://doi.org/10.1109/ISI53945.2021.9624765

[59] Ying Yuan, Giovanni Apruzzese, and Mauro Conti. 2023. Multi-SpacePhish: Extending the Evasion-space of Adversarial Attacks against Phishing Website Detectors using Machine Learning. *Digital Threats* (December 2023). DOI:https://doi.org/10.1145/3638253